Interferora Seach & updated Seach

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	0	encrypt\$3.clm, and radio.clm, and transmi\$4.clm, and authenticat\$3. clm, and network.clm, and access. clm, and subscriber.clm, and "private key".clm, and mobile.clm, and station.clm, and decipher\$.clm, and interface.clm.	USPAT	OR	OFF	2006/03/11 14:37
L2	11	encrypt\$3 and radio and transmi\$4 and authenticat\$3 and network and access and subscriber and "public key" and "private key" and mobile and station and decipher\$ and interface	USPAT	OR	OFF	2006/03/11 14:38
L3	14	encrypt\$3 and radio and transmi\$4 and authenticat\$3 and network and access and subscriber and "public key" and "private key" and mobile and station and decipher\$ and interface	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/03/11 14:38
L4	283	380/283	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/03/11 14:38
L5	7391	380/270 or 726/27 or 713/201	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/03/11 14:39
L6	7583	5 or 4	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/03/11 14:39
L7	3	6 and 3	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/03/11 14:43

EAST Search History

L8	583512	359/109 or "370" or "375" or "455" or 726/2	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/03/11 14:43
L9	8	8 and 3	US-PGPUB;	OR	OFF	2006/03/11 14:43
			USPAT;			
			USOCR;			
			EPO; JPO;			
			DERWENT;			
			IBM_TDB			

3/11/06 2:47:57 PM C:\Documents and Settings\KZand\My Documents\EAST\Workspaces\default.wsp



Subscribe (Full Service) Register (Limited Service, Free) Login

Search: • The ACM Digital Library • The Guide

encrypt\$3 and radio and transmi\$4 and authenticat\$3 and net



Relevance scale

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction surve

Terms used encrypt\$3 and radio and transmi\$4 and authenticat\$3 and network and access and subscriber and public 9,8 key and private key and mobile and station and decipher\$ and interface

Sort results by relevance

Save results to a Binder 2 Search Tips

Try an Advanced Search Try this search in The ACM Guide

Display results expanded form

Open results in a new window

Results 1 - 20 of 200

Result page: 1 2 3 4 5 6 7 8 9 10

Best 200 shown

Untraceability in mobile networks Didier Samfat, Refik Molva, N. Asokan

December 1995 Proceedings of the 1st annual international conference on Mobile computing and networking

Publisher: ACM Press

Full text available: pdf(1.20 MB)

Additional Information: full citation, references, citings, index terms

Keywords: CDPD, GSM, alias, anonymity, authentication, location privacy, mobility, security

Security issues for wireless ATM networks

Danai Patiyoot

January 2002 ACM SIGOPS Operating Systems Review, Volume 36 Issue 1

Publisher: ACM Press

Full text available: pdf(1.75 MB)

Additional Information: full citation, abstract, references, index terms

To be able to fulfil the need of user in wireless ATM, the system has to acquire features. One of the system features for the wireless ATM is functionality especially the security aspect. There is so far tittle, if not none, security consideration in the developing of wireless ATM standard. Therefore a wide range of features in security functions is in consideration. This paper tried to define the features of security in wireless ATM networks considering it features from existing fixed ATM netwo ...

Keywords: security, wireless ATM

3 Cryptographic security Techniques for wireless networks

Danai Patiyoot, S. J. Shepherd

April 1999 ACM SIGOPS Operating Systems Review, Volume 33 Issue 2

Publisher: ACM Press

Full text available: pdf(1.12 MB)

Additional Information: full citation, abstract, index terms

This paper deals with security techniques for wireless Networks. The work presented is based on a review of literature regarding current and future wireless security networks systems. The aspects discussed in this paper included the choices of cryptographic algorithms such as protocols for key management and authentication. Various conclusions are drawn from existing security networks and proposed in new wireless ATM network security. Also a proposal for future research into security techniques ...

Keywords: cryptographic, security, wireless

4 Best poster papers from MobiHoc 2002: Virtual operator based AAA in wireless LAN hot

spots with ad-hoc networking support

Junbiao Zhang, Jun Li, Stephen Weinstein, Nan Tu

June 2002 ACM SIGMOBILE Mobile Computing and Communications Review, Volume 6 Issue 3

Publisher: ACM Press

Full text available: pdf(180.11 KB)

Additional Information: full citation, abstract, references, citings, index terms

Sound and effective authentication, authorization and accounting (AAA) schemes for convenient and secure mobile wireless accesses are of great importance given the increased popularity and business opportunities in public wireless LAN hot spots. One possible scheme, which uses the mobile users' service providers as the single point of contact for all AAA transactions, is emerging as a very promising solution. We refer to such service providers as "virtual operators". In this paper, we discuss va ...

5 DRM experience: Digital rights management in a 3G mobile phone and beyond

Thomas S. Messerges, Ezzat A. Dabbish

October 2003 Proceedings of the 3rd ACM workshop on Digital rights management DRM '03

Publisher: ACM Press

Full text available: pdf(306.59 KB)

Additional Information: full citation, abstract, references, citings, index terms

In this paper we examine how copyright protection of digital items can be securely managed in a 3G mobile phone and other devices. First, the basic concepts, strategies, and requirements for digital rights management are reviewed. Next, a framework for protecting digital content in the embedded environment of a mobile phone is proposed and the elements in this system are defined. The means to enforce security in this system are described and a novel "Family Domain" approach to content management ...

Keywords: MPEG-21, copyright protection, cryptography, digital content, digital rights management, embedded system, key management, mobile phone, open mobile alliance, security

⁶ Security analysis: Privacy enhanced cellular access security

Geir M. Køien

September 2005 Proceedings of the 4th ACM workshop on Wireless security WiSe '05

Publisher: ACM Press

Full text available: pdf(230.28 KB)

Additional Information: full citation, abstract, references, index terms

The 3G cellular access security architectures do not provide satisfactorily user privacy and fail to fully include all three principal entities involved in the security context. In this paper we propose a beyond-3G Privacy Enhanced 3-Way Authentication and Key Agreement (PE3WAKA) protocol that provides substantially improved user privacy and a 3-way security context. By integrating selected Mobility Management procedures and the PE3WAKA protocol this is achieved with fewer round-trips than the 3 ...

Keywords: access security, entity authentication, wireless privacy

Bazaars, services, and systems: MoB: a mobile bazaar for wide-area wireless services Rajiv Chakravorty, Sulabh Agarwal, Suman Banerjee, Ian Pratt



August 2005 Proceedings of the 11th annual international conference on Mobile computing and networking MobiCom '05

Publisher: ACM Press

Full text available: pdf(344.72 KB) Additional Information: full citation, abstract, references, index terms

We introduce MoB, an infrastructure for collaborative wide-area wireless data services. MoB proposes to change the current model of data services in the following fundamental ways: (1) it decouples infrastructure providers from services providers and enables fine-grained competition, (2) it allows service interactions on arbitrary timescales, and, (3) it promotes flexible composition of these fine-grained service interactions based on user and application needs. At the heart of MoB is an open mar ...

Keywords: incentives, reputation, wide-area wireless, wireless services

Mobile computing and applications (MCA): Delivering Attribute Certificates over GPRS

Georgios Kambourakis, Angelos Rouskas, Stefanos Gritzalis

March 2004 Proceedings of the 2004 ACM symposium on Applied computing

Publisher: ACM Press

Full text available: pdf(182.76 KB) Additional Information: full citation, abstract, references, index terms

Attribute Certificates (ACs) have been developed and standardized by the ANSI X9 committee as an alternative and better approach, to X.509 public key certificates, for carrying authorization information. Attribute Authorities (AA) bind the characteristics of an entity (called attributes) to that entity by signing the appropriate AC. Therefore, ACs can be used for controlling access to system resources and employing role-based authorization and access controls policies accordingly. Although ACs a ...

Keywords: GPRS, PKI, UMTS, attribute certificates, performance evaluation

Security in mobile communications: challenges and opportunities Audun Jøsang, Gunnar Sanderud

January 2003 Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003 - Volume 21 CRPITS '03

Publisher: Australian Computer Society, Inc.

Full text available: pdf(117.04 KB) Additional Information: full citation, abstract, references, citings, index terms

The nature of mobile communication, characterised for example by terminals having poor user interface and limited processing capacity, as well as complex combination of network protocols, makes the design of security solutions particularly challenging. This paper discusses some of the difficulties system architects are faced with as well as some advantages mobile networks offer when designing security solutions for mobile communication.

Keywords: heterogeneous networks, mobile devices, security, usability

10 Authentication protocols for personal communication systems

Hung-Yu Lin, Lein Harn

October 1995 ACM SIGCOMM Computer Communication Review , Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communication SIGCOMM '95, Volume 25 Issue 4

Publisher: ACM Press

Full text available: pdf(647.17 KB) Additional Information: full citation, abstract, references, citings, index terms

Masquerading and eavesdropping are major threats to the security of wireless communications. To provide proper protection for the communication of the wireless link, contents of the

communication should be enciphered and mutual authentication should be conducted between the subscriber and the serving network. Several protocols have been proposed by standards bodies and independent researchers in recent years to counteract these threats. However, the strength of these protocols is usually weakene ...

11 Accounting and management: Generic accounting configuration management for

heterogeneous mobile networks

Frank Eyermann, Peter Racz, Burkhard Stiller, Christian Schaefer, Thomas Walter September 2005 Proceedings of the 3rd ACM international workshop on Wireless mobile applications and services on WLAN hotspots WMASH '05

Publisher: ACM Press

Additional Information: full citation, abstract, references, index terms Full text available: pdf(252.81 KB)

Accounting performed by network and service providers covers the tasks of determining, collecting, and evaluating information on the service usage of their customers. This information forms the basis of the subsequent charging process. For performing these tasks in case of heterogeneous mobile networks a generic configuration management, specifically tailored at the provisioning of various Internet services is needed. This work defines a role model covering all participating entities of a distri ...

Keywords: accounting, accounting architecture, charging, hand-over, mobile network operators, roaming, single bill

12 Secure services: JANUS: towards robust and malicious resilient routing in hybrid wireless

networks

Bogdan Carbunar, Ioanis Ioannidis, Cristina Nita-Rotaru

October 2004 Proceedings of the 2004 ACM workshop on Wireless security

Publisher: ACM Press

Full text available: pdf(169,26 KB) Additional Information: full citation, abstract, references, index terms

In this paper we investigate and provide solutions for security threats in the context of hybrid networks consisting of a cellular base station and mobile devices equipped with dual cellular and ad-hoc (802.11b) cards. The cellular connection is used for receiving services (i.e. Internet access) from the base station, while the ad-hoc links are used to improve the quality of the connection. We provide detailed descriptions of several attacks that arbitrarily powerful adversaries, whether outside ...

Keywords: hybrid wireless networks, routing, security

13 Security Mechanisms in High-Level Network Protocols

Victor L. Voydock, Stephen T. Kent

June 1983 ACM Computing Surveys (CSUR), Volume 15 Issue 2

Publisher: ACM Press

Full text available: pdf(3,23 MB) Additional Information: full citation, references, citings

14 New basic technologies for DIM: Pseudonym management using mediated identity-based

Thibault Candebat, Cameron Ross Dunne, David T. Gray

November 2005 Proceedings of the 2005 workshop on Digital identity management DIM

Publisher: ACM Press

Full text available: pdf(293,16 KB) Additional Information: full citation, abstract, references, index terms Mobile Location-Based Services (LBS) have raised privacy concerns amongst mobile phone users who may need to supply their identity and location information to untrustworthy third parties in order to access these applications. Widespread acceptance of such services may therefore depend on how privacy sensitive information will be handled in order to restore users' confidence in what could become the "killer app" of 3G networks. In this paper, we present a proxy-based public key infrastructure tha ...

Keywords: SEM architecture, identity-based encryption, location-based services, pseudonymity

15 Distributed PIN verification scheme for improving security of mobile devices

Jian Tang, Vagan Terziyan, Jari Veijalainen

April 2003 Mobile Networks and Applications, Volume 8 Issue 2

Publisher: Kluwer Academic Publishers

Full text available: pdf(298.43 KB) Additional Information: full citation, abstract, references, index terms

The main driving force for the rapid acceptance rate of small sized mobile devices is the capability to perform e-commerce transactions at any time and at any place, especially while or the move. There are, however, also weaknesses of this type of e-commerce, often called mobile e-commerce, or m-commerce. Due to their small size and easy portability mobile devices can easily be lost or stolen. Whereas the economic values and privacy threats protected with Personal Identification Numbers (PIN) ar ...

Keywords: measure, mobile device, probability, risks, security, uncover

16 Invited workshop on network security and management: Security protocols for 2G and 3G wireless communications

T. Newe, T. Coffey

September 2003 Proceedings of the 1st international symposium on Information and communication technologies ISICT '03

Publisher: Trinity College Dublin

Full text available: pdf(190.85 KB) Additional Information: full citation, abstract, references

Wireless communications are being driven by the need for providing network access to mobile or nomadic computing devices. The need for wireless access to a network is evident in current work environments. A number of new protocols have been recently published with the goal of providing both privacy of data and authentication of users for mobile systems. Such protocols can employ private-key and/or public key cryptographic algorithms. Publickey algorithms hold the promise of simplifying the netwo ...

Keywords: 2G, 3G, end-to-end, mobile, radio-link, security

17 The Satchel system architecture: mobile access to documents and services Mike Flynn, David Pendlebury, Chris Jones, Marge Eldridge, Mik Lamming December 2000 Mobile Networks and Applications, Volume 5 Issue 4

Publisher: Kluwer Academic Publishers

Full text available: pdf(207.51 KB) Additional Information: full citation, abstract, references, citings, index terms

Mobile professionals require access to documents and document‐ related services, such as printing, wherever they may be. They may also wish to give documents to colleagues electronically, as easily as with paper, face‐to‐face, and with similar security characteristics. The Satchel system provides such capabilities in the form of a mobile browser, implemented on a device that professional people would be likely to carry anyway, such as a

pager or mobile phone. Printing may be per ...

18 Link and channel measurement: A simple mechanism for capturing and replaying wireless

<u>channels</u>

Glenn Judd, Peter Steenkiste

August 2005 Proceeding of the 2005 ACM SIGCOMM workshop on Experimental approaches to wireless network design and analysis E-WIND '05

Publisher: ACM Press

Full text available: pdf(6.06 MB)

Additional Information: full citation, abstract, references, index terms

Physical layer wireless network emulation has the potential to be a powerful experimental tool. An important challenge in physical emulation, and traditional simulation, is to accurately model the wireless channel. In this paper we examine the possibility of using on-card signal strength measurements to capture wireless channel traces. A key advantage of this approach is the simplicity and ubiquity with which these measurements can be obtained since virtually all wireless devices provide the req ...

Keywords: channel capture, emulation, wireless

19 Enhanced privacy and authentication for the global system for mobile communications

Chii-Hwa Lee, Min-Shiang Hwang, Wei-Pang Yang July 1999 **Wireless Networks**, Volume 5 Issue 4

Publisher: Kluwer Academic Publishers

Full text available: pdf(204.97 KB)

Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>citings</u>, <u>index terms</u>,

The Global System for Mobile Communications (GSM) is widely recognized as the modern digita mobile network architecture. Increasing market demands point toward the relevancy of security-related issues in communications. The security requirements of mobile communications for the mobile users include: (1) the authentication of the mobile user and Visitor Location Register/Home Location Register; (2) the data confidentiality between mobile station and Visitor Location Register, and the data c ...

20 Verifying security protocols as planning in logic programming

Luigia Carlucci Aiello, Fabio Massacci

October 2001 ACM Transactions on Computational Logic (TOCL), Volume 2 Issue 4

Publisher: ACM Press

Full text available: pdf(305.94 KB)

Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>citings</u>, <u>index terms</u>, <u>review</u>

We illustrate ALSP (Action Language for Security Protocol), a declarative executable specification language for planning attacks to security protocols. ALSP is based on logic programming with negation as failure, and with stable model semantics. In ALSP we can give a declarative specification of a protocol with the natural semantics of send and receive actions which can be performed in parallel. By viewing a protocol trace as a plan to a ...

Keywords: AI planning, logic programming, security protocols, specification language

Results 1 - 20 of 200 Result page: 1 2 3 4 5 6 7 8 9 10 next

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2006 ACM, Inc.

Terms of Usage Privacy Policy Code of Ethics Contact Us

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player